AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A system for securing an application for execution on a computer, the system comprising:

a preprocessor module for identifying calls that are made by ~~the~~ an application binary to at least one routine that is provided by an operating system, the preprocessor module, prior to execution of the application binary, modifying the application binary such that an interception module is invoked in response to the application binary invoking the identified ~~routines~~ calls;

a server computer for receiving at least one application binary that has been modified by the preprocessor module;

a network; and

a client computer operably connected to the server computer via the network, wherein the client computer receives from the server computer a modified application binary, wherein subsequent to receiving the modified application binary, the client computer executes the modified application binary.

2. (Currently Amended) A method of securing an application ~~for execution on a computer~~, the method comprising:

prior to execution of the application program, scanning the application program for code sequences that cause ~~the~~ a computer to trap to the operating system;

prior to execution of the application program, modifying the code sequences such that the computer does not trap to the operating system;

prior to execution of the application program, identifying at least one call that are made by the application to an external routine;

prior to execution of the application program, providing at least one interception module for the identified calls; and

prior to execution of an application program, storing the modified application program~~;~~

~~transmitting the application program and the at least one interception module to the computer;~~

~~intercepting at least one of the identified calls at the computer;~~

~~monitoring at the computer the usage of resources by the computer; and~~

~~preventing the application from consuming resources in excess of a predefined threshold~~.

3. (Currently Amended) A method of securing an application ~~for execution on a computer~~, the method comprising:

scanning the application program for code sequences that cause the computer to trap to the operating system;

modifying the code sequences such that the computer does not trap to the operating system;

identifying at least one call that is made by the application to an external routine;

providing at least one interception module for the identified calls;

storing the modified application program and the interception module~~;~~

~~transmitting the application program to the computer; and~~

~~intercepting at least one of the identified calls at the computer~~.

4. (Currently Amended) A method of securing an application for execution on a computer, the method comprising:

identifying calls that are made by the application to an external routine, wherein the application includes at least one binary;

prior to execution of the application, modifying the binary ~~of an application~~ to invoke an interception module; and

storing the modified binary ~~intercepting at least one of the identified calls at the computer~~.

5. (Original) The method of Claim 4, additionally comprising transmitting the application and at least one interception module to the computer.

6. (Currently Amended) A method of securing an application ~~for execution on a computer~~, the method comprising:

identifying calls that cause a detrimental effect to the computer or another application;

prior to execution of the calls, modifying a binary of the application to invoke an interception module with respect to the identified calls; and

storing the modified binary~~; and~~

~~intercepting at least one of the identified calls~~.

7. (Currently Amended) A method of securing an application ~~for execution on a computer~~, the method comprising:

intercepting at least one call that is made by the application such that a graphical user interface that is displayed by the application is modified;

intercepting at least one call that is made by the application program such that requests for machine or user specific information are virtualized; and

intercepting at least one call that is made by the application such that the contents of at least one file that is used by the application is encrypted transparently to the application.

8. (Original) The method of Claim 7, wherein the machine information includes operating system information.

9. (Original) The method of Claim 7, additionally comprising intercepting at least one call that is made by the application such that the filename of at least one file that is used by the application is encrypted transparently to the application.

10. (Original) The method of Claim 7, additionally comprising modifying a directory structure of a set of files.

11. (Currently Amended) A method of securing an application ~~for execution on a computer~~, the method comprising:

intercepting at least one call that is made by the application such that a graphical user interface that is displayed by the application is modified; and

intercepting at least one call that is made by the application such that the contents of at least one file that is used by the application is encrypted transparently to the application.

12. (Original) The method of Claim 11, additionally comprising intercepting at least one call that is made by the application such that the filename of at least one file that is used by the application is encrypted transparently to the application.

13. (Original) The method of Claim 11, additionally comprising modifying a directory structure of a set of files.

14. (Original) A program storage device storing instructions that when executed perform the steps comprising:

intercepting at least one call that is made by the application such that a graphical user interface that is displayed by the application is modified; and

intercepting at least one call that is made by the application such that the contents of at least one file that is used by the application is encrypted transparently to the application.

15. (Currently Amended) A method for allowing application programs to execute in non-native environments, the method comprising:

identifying a service that is not provided by a selected operating system; and

prior to execution of an application program, modifying a binary of ~~an~~ the application program to invoke an interception service instead of requesting the service from the selected operating system.

16. (Cancelled).

17. (Cancelled).

18. (Cancelled).

19. (Cancelled).

20. (Currently Amended) A system for securing an application ~~for execution on a computer~~, the system comprising:

means for scanning the application program for code sequences that cause the computer to trap to the operating system;

means for, prior to execution of the application program, modifying the code sequences such that the computer does not trap to the operating system;

means for identifying calls that are made by the application to an external routine;

means for providing at least one interception module for the identified calls;

means for storing the modified code sequences; and

means for transmitting the application program and the at least one interception module to the computer~~;~~

~~means for intercepting at least one of the identified calls at the computer;~~

~~means for monitoring at the computer the usage of resources by the computer; and~~

~~means for preventing the application from consuming resources in excess of a threshold~~.

21. (Original) The system of Claim 20, wherein the threshold is determined in real time by monitoring the system state.

22. (Currently Amended) A system for securing an application ~~for execution on a computer~~, the system comprising:

means for scanning the application program for code sequences that cause the computer to trap to the operating system;

means for, prior to execution of the application program, modifying the code sequences such that the computer does not trap to the operating system;

means for identifying calls that are made by the application to an external routine;

means for providing at least one interception module for the identified calls; and

means for storing the modified code sequences

~~means for transmitting the application program to the computer; and~~

~~means for intercepting at least one of the identified calls at the computer~~.

23. (Currently Amended) The system of Claim 22, additionally comprising ~~wherein the~~ means for intercepting at least one of the ~~identifies~~ identified calls and wherein the means for intercepting prevents the application from communicating with network devices that are not listed in a pre-approved list of network connections.

24. (Cancelled)

25. (Currently Amended) A system for securing an application ~~for execution on a computer~~, the system comprising:

means for intercepting at least one call that is made by the application such that a graphical user interface that is displayed by the application is modified;

means for intercepting at least one call that is made by the application program such that requests for machine or user information are virtualized; and

means for intercepting at least one call that is made by the application such that the contents of at least one file that is used by the application is encrypted transparently to the application.

26. (Original) The system of Claim 25, additionally comprising means for intercepting at least one call that is made by the application such that the filename of at least one file that is used by the application is encrypted transparently to the application.

27. (Original) The system of Claim 25, additionally comprising means for modifying a directory structure of a set of files.

28. (Original) A system for securing an application for execution on a computer, the system comprising:

means for intercepting at least one call that is made by the application such that a graphical user interface that is displayed by the application is modified; and

means for intercepting at least one call that is made by the application such that the contents of at least one file that is used by the application is encrypted transparently to the application.

29. (Original) The system of Claim 28, additionally comprising intercepting at least one call that is made by the application such that the filename of at least one file that is used by the application is encrypted transparently to the application.

30. (Original) The system of Claim 28, additionally comprising means for modifying a directory structure of a set of files.

31. (Cancelled)

32. (Cancelled)

33. (Cancelled).

34. (Cancelled).

35. (Currently Amended) A system for securing an application ~~for execution on a computer~~, the system comprising:

a preprocessor module for, prior to execution of the application, identifying calls that are made by the application to at least one external routine, the preprocessor module modifying the application to invoke an interception module in response to the application invoking the external routine, the preprocessor module configured to store the modified application.

36. (Original) The system of Claim 35, wherein the preprocessor module encrypts at least a portion of a filename that is associated with the application.

37. (Original) The system of Claim 35, wherein the preprocessor module encrypts the contents of at least a portion of the application.

38. (Original) A method of securing an application for execution on a computer, the method comprising:

rewriting the binary of an application thereby preventing the application from: accessing a predefined set of data; invoking a predefined set of instructions; and accessing one or more files that are in one or more predefined directories.

39. (Original) The method of Claim 38, additionally comprising rewriting the binary of the application thereby preventing the application from modifying an output device of the computer.